REMARKS

In the Non-Final Office Action dated April 22, 2004, claims 1-20 are pending. Claims 1 and 10 are independent claims from which all other claims depend therefrom. Claims 1 and 10 have been amended. Note that claims 1 and 10 have not been amended for patentability reasons but rather for clarification reasons.

Claims 1 and 10 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Preston et al. (U.S. Publication No. 2002/0032853), in view of Willis et al. (U.S. Patent No. 6,385,647).

Claims 1 and 10 have similar limitations and are therefore discussed together. Claim 1 recites a virtual biological fluid system for secure communications. The system includes a primary gateway having security information and multiple communication layers. A security control plane is formed using information from each of the communication layers. The control plane in conjunction with the security information forms a virtual biological fluid insuring secure data transmission. Claim 10 recites a method for secure communications over a network. Claim 10 has similar limitations to that of claim 1.

The integrating of information from each of the communication layers into a secure control plane is more effective than any individual security protocol. This integration provides an improved and reliable secure communication system for various communication networks. Also, the use of a security control plane in conjunction with a station containing security information to form a biological fluid enables the use of an interactive security doctrine that allows for multiple levels of security deployment.

Preston discloses a secure dynamic link allocation system for mobile data communication. The Office Action states that Preston discloses a security control plane formed using information from multiple communication layers. The Office Action refers to the security manager of Preston as the security control

plane. Applicant respectfully traverses. Although Preston may disclose the use of multiple communication layers, Preston only discloses the use of information from a single communication layer, namely the session layer. As shown in Figure 1 of Preston, the session layer is coupled to the security manager. All other layers of communication are not coupled to nor do they provide information to the security manager. In comparing Figure 1 with that of Figure 2 of the present application one can quickly and easily see the difference in the configurations between the system of Preston and that of the present application. The security manager of Preston is in communication with the session layer, whereas the system and method of claims 1 and 10 of the present application provide communication between a security plane and multiple communication layers, as is illustrated as an example in Figure 2.

In addition, Preston does not teach or suggest the use of a security control plane, as described above, in conjunction with security information to form a virtual biological fluid. The security manager of Preston uses a key and encryption for security, see paragraph [0016] and Figures 2A, 2B, and 3 of Preston. The use of a key, as stated in the background section of the present application, does not protect against eavesdropping and data gathering and post processing. The use of a key also does not allow a system to detect a breach in security and may allow for computation sharing for key acquisition. The Office Action states that Preston discloses a system for layered and secured data communication. Applicant submits that the key and encryption of Preston are utilized in a single layer, the session layer.

The Office Action further states that Preston does not expressly disclose a primary gateway having security information. Applicant agrees. However the Office Action states that Willis discloses a primary gateway having security information.

Willis discloses a system for selectively routing data via either network that supports internet protocol or via satellite transmission network based on size of the data. Although Willis may disclose the use of a gateway having secured

information, Willis like Preston does not teach or suggest a security control plane formed using information from multiple communication layers or the use of a security control plane in conjunction with security information to form a virtual biological fluid.

Applicant now refers to MPEP 706.02(j) and submits that to establish a *prima facie* case of obviousness the prior art references must teach or suggest all the claim limitations. As stated above, all of the claimed limitations of claims 1 and 10 are not taught or suggested by Preston or Willis.

Referring to MPEP § 2143.01, the fact that references can be combined or modified is not sufficient to establish *Prima Facie* obviousness, the prior art must also suggest the desirability of the combination and the modification, *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). None of the references suggest such combination and clearly none of the references suggest performing some sort of combination and modification thereof to arrive at the system and method of claims 1 and 10.

Additionally, referring to MPEP 2141.01(a), while the Patent Office classification of references and cross-references in the official search notes are some evidence of "nonanalogy" or "analogy" respectively, the court has found "the similarities and differences in structure and function of the inventions to carry far greater weight." *In re Ellis*, 476 F.2d 1370, 1372, 177USPQ526, 527 (CCPA 1973). Willis would not have logically commended itself to an inventor's attention in considering the problems solved by the system and method of claims 1 and 10. In developing a satellite system for secured communication, one would clearly not look to a method for selectively routing data based on the size of the data. Willis is directed to the efficiency of data communication not the security thereof. Although Willis mentions that a secure transfer protocol may be used, Willis does not describe the operation, functioning, or configuration of a security system. The system of Willis would not have logically commended itself to the Applicant's attention in solving the problems associated with secure communication. Willis would not be reasonably pertinent to the particular

problems solved by the system and method of claims 1 and 10. Thus, the Applicant submits that Willis is nonanalogous art.

Applicant submits that since the rejections with respect to claims 1 and 10 have been overcome that claims 1 and 10 are novel, nonobvious, and are in a condition for allowance.

Claims 2-9 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Preston and Willis in view of Greene (U.S. Patent No. 6,578,145).

Applicant submits that since claims 2-9 depend from claim 1, claims 2-9 are novel, nonobvious, and are in a condition for allowance for at least the same reasons as put forth above with respect to claim 1.

Greene discloses a system for securely communicating personal identification number information between a security module and multiple security keypad devices. Applicant submits that Greene as with Preston and Willis also fails to teach or suggest a security control plane formed using information from multiple communication layers or the use of a security control plane in conjunction with security information to form a virtual biological fluid.

In light of the amendments and remarks, Applicant submits that all rejections are now overcome. The Applicant has added no new matter to the application by these amendments. The application is now in condition for allowance and expeditious notice thereof is earnestly solicited. Should the Examiner have any questions or comments, he is respectfully requested to call the undersigned attorney.

Respectfully submitted,

July 19 2004

Georgann S. Grunebach
Reg. No. 33,179
Attorney for Applicants

Date: July 19, 2004

The DirecTV Group, Inc.
RE / R11 / A109
2250 East Imperial Highway
P.O. Box 956
El Segundo, CA 90245
Telephone: (310) 964-4615